AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently amended) A content management method for managing content data provided to user equipment, comprising the steps of:

storing a content key encrypted with a first storage key, content data encrypted with the content key, and a second storage key in the user equipment;

sending the encrypted content key and the second storage key to a key management unit;

at the key management unit, decrypting the encrypted content key using the first storage key, the first storage key being stored in the key management unit; ~~and~~

encrypting the decrypted content key using the second storage key;

sending the content key encrypted with the second storage key ~~along with the encrypted content~~ to the user equipment; and

at the user equipment, decrypting the encrypted content key using the second storage key and decrypting the content data using the decrypted content key.

2. (Original) The method as set forth in Claim 1, wherein the second storage key is generated based on a random number.

3. (Previously presented) The method as set forth in Claim 1, wherein the decrypted content key is encrypted with identification information of the user equipment and stored into the user equipment.

4. (Previously presented) The method as set forth in Claim 1, wherein the content key is encrypted, in the user equipment, with the first storage key and identification information of the user equipment, and the content key stored in the user equipment is decrypted with the first storage key and the identification information of the user equipment.

5. (Previously presented) The method as set forth in Claim 1, wherein the second storage key is generated by a decrypted key generating means provided in the user equipment.

6. (Previously presented) The method as set forth in Claim 5, wherein the second storage key is encrypted with a public key for the key management unit for management of the storage keys to generate a third storage key and the third storage key is stored into the user equipment.

7. (Previously presented) The method as set forth in Claim 6, wherein the user equipment deletes the second storage key depending upon whether the third storage key has been stored in the user equipment.

8. (Previously presented) The method as set forth in Claim 7, wherein, when decrypting the content key stored in the user equipment, the user equipment sends the third storage key to the key management unit; and the key management unit generates

the second storage key based on the third storage key while performing an accounting following a predetermined procedure.

9. (Previously presented) The method as set forth in Claim 1, wherein the second storage key is generated by a storage key generating means provided in the key management unit which manages the storage keys; and the key management unit has stored therein the second storage key and identification information of the user equipment in which the content key encrypted with the above generated second storage key is stored.

10. (Previously presented) The method as set forth in Claim 9, wherein upon the generation of the second storage key, the key management unit performs an accounting following a predetermined procedure.

11. (Previously presented) The method as set forth in Claim 9, wherein the key management unit encrypts the second storage key with the management key to generate a third storage key, and sends the third storage key to the user equipment; and the user equipment stores the received third storage key.

12. (Previously presented) The method as set forth in Claim 11, wherein the user equipment deletes the second storage key depending upon whether the third storage key has been stored.

13. (Previously presented) The method as set forth in Claim 12, wherein the key management unit has stored therein the identification information of the user equipment in which the content key encrypted with the second storage key is stored; the user equipment sends, when decrypting the content key stored in the user equipment, the identification information of the user equipment to the key management unit; and the key management unit generates the second storage key based on the result of comparison between identification information of the user equipment, sent from the user equipment, and the identification information of the user equipment, held in the key management unit itself, while accounting the data service following the predetermined procedure.

14. (Previously presented) The method as set forth in Claim 1, wherein the user equipment has stored therein identification information of the user equipment.

15. (Previously presented) The method as set forth in Claim 14, wherein the user equipment starts decrypting the content key stored in the user equipment depending upon the result of an inspection of the identification information of the user equipment, stored in the user equipment.

16. (Previously presented) The method as set forth in Claim 1, wherein the decrypted content key supplied from the user equipment has added thereto information that the content key has been obtained by restoration.

17. (Previously presented) The method as set forth in Claim 16, wherein when moving the content key having added thereto the information that the content key has been obtained by restoration, the user equipment performs an error process based on the result of comparison between the content key and another content key stored in a destination to which the content key is to be moved.

18. (Previously presented) The method as set forth in Claim 1, wherein the content key has added thereto frequency information that limits the number of times the content key can be used.

19. (Previously presented) The method as set forth in Claim 1, further comprising storing the content key encrypted with the second storage key in a first storage of the user equipment along with identification information of the first storage; storing the content key that is stored in the first storage, and the identification information of the first storage, into a second storage of the user equipment; and performing, when a request is made to decrypt the content key in the first storage, an error process based on the result of comparison between the identification information of the first storage and the identification information of the second storage.

20. (Previously presented) A content management system for managing content data, comprising:

a storing means having stored therein a content key encrypted with a first storage key, content data encrypted with the content key, and a second storage key;

a sending means for sending the encrypted content key and the second storage key to a key management unit;

a first decrypting means, in the key management unit, for decrypting the encrypted content key using the first storage key, the first storage key being stored in the key management unit;

an encrypting means for encrypting the decrypted content key using the second storage key; and

a second decrypting means for decrypting the encrypted content key using the second storage key and decrypting the content data using the decrypted content key.

21. (Previously presented) The system as set forth in Claim 20, further comprising storage key generating means for generating the second storage key by means of a random number generator.

22. (Previously presented) The system as set forth in Claim 20, wherein the encrypting means encrypts the decrypted content key with identification information of the storing means.

23. (Previously presented) The system as set forth in Claim 20, wherein the content key is encrypted, in the storing means, with the first storage key and identification information of the storing means; and the content key stored in the storing means is decrypted with the first storage key and the identification information of the storing means.

24. (Previously presented) The system as set forth in Claim 20, wherein the storing means, first decrypting means, and encrypting means form together a data storage, and wherein the key management unit manages the second storage key of the data storage.

25. (Previously presented) The system as set forth in Claim 24, wherein the data storage is a data receiver that receives a content data encrypted and sent from a data transmitter.

26. (Previously presented) The system as set forth in Claim 24, further comprising means for storing a public key of the key management unit; and wherein the storing means has stored therein the second storage key along with a third storage key obtained by encrypting the second storage key with the public key.

27. (Previously presented) The system as set forth in Claim 26, wherein the data storage deletes the second storage key depending upon whether the third storage key is stored in the storing means.

28. (Previously presented) The system as set forth in Claim 27, wherein, when decrypting the content key stored in the storing means, the data storage sends the third storage key to the key management unit; and the key management unit sends the second storage key generated based on the third storage key to a data transmitter while performing an accounting following a predetermined procedure.

29. (Previously presented) The system as set forth in Claim 24, wherein the storing means has stored therein identification information of the data storage.

30. (Previously presented) The system as set forth in Claim 29, wherein the data storage starts decrypting the content key stored in the storing means depending on the result of inspection of the identification information of the data storage, stored in the storing means.

31. (Previously presented) The system as set forth in Claim 20, wherein the storing means, first decrypting means, and encrypting means form together a data storage; and further comprising a storage key generating means, wherein the key management unit manages the second storage key of the data storage.

32. (Previously presented) The system as set forth in Claim 31, wherein the data storage is a data receiver that receives a content data encrypted and sent from a data transmitter.

33. (Previously presented) The system as set forth in Claim 31, wherein the key management unit comprises an identification information storing means in which identification information of the storing means is stored.

34. (Previously presented) The system as set forth in Claim 31, wherein the key management unit performs an accounting following a predetermined procedure depending upon a generation of the second storage key.

35. (Previously presented) The system as set forth in Claim 31, wherein the key management unit comprises means for storing storage keys; the key management unit generates a third storage key by encrypting the second storage key with a management key and sends the third storage key to the data storage; and the data storage stores the third storage key into the storing means.

36. (Previously presented) The system as set forth in Claim 35, wherein the data storage deletes the second storage key depending upon whether the third storage key is stored in the storing means.

37. (Previously presented) The system as set forth in Claim 36, wherein the key management unit comprises means for storing the second storage key and identification information of the storing means in which the content key encrypted with the second storage key is stored; the key management unit performs an accounting, when the data storage decrypts the content key, following a predetermined procedure based on the result of comparison between the identification information of the storing means, sent from the data storage, and identification information stored in an identification information storing means.

38. (Previously presented) The system as set forth in Claim 31, wherein the storing means has stored therein identification information of the data storage.

39. (Previously presented) The system as set forth in Claim 38, wherein the data storage starts decrypting the content key stored in the storing means.

40. (Previously presented) The system as set forth in Claim 20, wherein the content key obtained by decryption from the storing means has added thereto information that the content key has been obtained by restoration, as requirement information.

41. (Previously presented) The system as set forth in Claim 20, wherein the content key has added thereto frequency information that limits the number of times the content key can be used.